

Cybersecurity Foundations

Learn via: **Classroom / Virtual Classroom / Online**

Duration: **5 Gün**

<https://bilginc.com/tr/egitim/cybersecurity-foundations-1515-egitimi/>

Overview

Bu Cybersecurity Foundations eğitiminde, güvenli bir sistem tasarlamamanın zorlukları ve tutarlı bir güvenlik çözümü sağlamak için gereken bütün siber rollere değinen küresel bir bakış açısı kazanacaksınız. Konferans, laboratuvarlar ve toplu tartışma grupları aracılığıyla, Internet'teki mevcut tehdit eğilimleri ve bunların örgütsel güvenlik üzerindeki etkilerini öğreneceksiniz. Standart siber güvenlik terminolojisi ve uyumluluk gereksinimlerini gözden geçirecek, örnek istisnaları inceleyecek ve uygulamalı deneyim azaltıcı kontroller elde edeceksiniz. İçerilen laboratuvar ortamında, botnet, solucan ve Truva atı gibi canlı virüslerle çalışacaksınız.

Prerequisites

Katılımcılar TCP/IP ağı veya eşdeğer bilgiye sahip olmalıdır.

Who Should Attend

Bu eğitime, bilgilerini ilerletmek ve siber güvenliği bir kariyer yolu olarak keşfetmek isteyen ağ uzmanları; güvenlik uzmanlarıyla iletişim kurma yeteneklerini artırmak ve kurumsal düzeyde sağlam bir güvenlik çözümü uygulamak isteyen yöneticiler ve yetkililer; tehditler, hafifletici kontroller ve örgütsel sorumluluklar dahil siber güvenlik temellerini anlayıp kendini bu alanda geliştirmeyi isteyen bireyler katılmalıdır.

What You Will Learn

- Güvenlik bilincinizi arttırın.
- Ağ haritalama için araç çıktısını/ ayak izini yorumlama/ analiz etme
- Sistemlerin saldırı yüzeyini azaltın.
- Güvenlik denetimi uygulandığında ağı gözden geçirin.
- Farklı veri koruma ilkelerini keşfedin.
- Bir ağdaki cihazlar arasında güvenilir ilişkiler oluşturmada PKI / sertifikaların rolünü inceleyin.
- Giriş güvenliği ve diğer kimlik yönetimi çözümlerini uygulayın.
- Ağ cihazlarının saldırı yüzeyini azaltın.
- Mevcut kötü amaçlı yazılım tehditlerini ve kötü amaçlı yazılımdan korunma çözümlerini keşfedin.
- Sosyal mühendislik tehditlerini, yöntemlerini ve tekniklerini keşfedin.
- Sömürü riskini azaltmak için yazılım açıklarını ve güvenlik çözümlerini inceleyin.
- İzleme kapasitesini ve gereksinimlerini, bunların gizlilik endişelerini nasıl arttırabileceğini açıklayın.
- Fiziksel güvenlik kontrollerini ve fiziksel ile IT güvenliği arasındaki ilişkiyi tanımlayın.
- Olay müdahale yeteneklerini açıklayın.
- Siber güvenlik söz konusu olduğunda yasal hususları ve soruşturma tekniklerini belirleyin.
- Siber güvenlik alanında araştırma eğilimleri

Outline

1. Siber Güvenlik Bilinci

- Güvenlik Nedir?
- Gizlilik, Bütünlük ve Kullanılabilirlik
- Güvenlik Taban Çizgisi
- Güvenlik Endişeleri: İnsanlar

- Tehdit Türleri
- Güvenlik Kontrolleri
- Hack Nedir?
- Risk Yönetimi
- Hareket Halindeki Veriler ve Hareketsiz Veriler
- Modül İncelemesi

2. Ağ Keşfi

- Ağ İncelemesi
- Keşif, Ayak izi ve Tarama
- Ortak Güvenlik Açıkları ve Riskler
- Güvenlik Politikaları
- Güvenlik Açıkları
- Modül İncelemesi

3. Sistem Sağlamaştırma

- Sertleşme Nedir?
- Sertleştirilebilecek Sistem Tipleri
- Güvenlik Taban Çizgileri
- Sistemler Nasıl Sağlamaştırma
- Sertleştirme Sistemleri Rolü
- Mobil Cihazlar
- Ağda Sağlamaştırma
- Analiz Araçları
- Kimlik Doğrulama, Yetkilendirme ve Muhasebe
- Fiziksel Güvenlik
- Modül İncelemesi

4. Güvenlik Mimarisi

- Güvenlik Mimarisi
- Ağ Cihazları
- Ağ Bölgeleri
- Ağ Bölümlendirme
- Ağ Adresi Çevirisi
- Ağ Erişim Kontrolü
- Modül İncelemesi

5. Veri Güvenliği

- Kriptografi
- İzin İlkeleri
- Steganografi
- Modül İncelemesi

6. Genel Anahtar Altyapısı

- Açık Anahtar Altyapısı
- Sertifika Yetkilileri
- Güveni Etkinleştirmek
- Sertifikalar
- CA Yönetimi
- Modül İncelemesi

7. Kimlik Yönetimi

- Kimlik Yönetimi Nedir?
- Kişisel Olarak Tanımlanabilir İlgiler
- Kimlik Doğrulama Faktörleri
- Rehber Hizmetleri
- Kerberos
- Windows NT LAN Yöneticisi
- Şifre Politikaları
- Şifreleri Kırma
- Şifre Değerlendirme araçları
- Şifre Yöneticileri
- Grup Hesapları
- Hizmet Hesapları
- Birleşik Kimlikler
- Hizmet Olarak Kimlik
- Modül İncelemesi

8. Ağ Sağlamaştırma

- Uzaktan Yönetici Erişimini Sınırlama
- AAA: İdari erişim
- Basit Ağ Yönetimi Protokolü
- Ağ Bölümlendirme
- Fiziksel Erişimi Sınırlamak
- Güvenli Erişim Kurmak
- Ağ Cihazları
- Temel Cihaz Koruma Özeti
- Trafik Filtreleme En İyi Uygulamaları
- Modül İncelemesi

9. Kötü Amaçlı Yazılım

- Kötü Amaçlı Yazılım Nedir?
- Enfeksiyon Yöntemleri
- Kötü Amaçlı Yazılım Türleri
- Arkakapılar
- Karşı Önlem
- Koruma Araçları
- Modül İncelemesi

10. Sosyal Mühendislik

- Sosyal Mühendislik Nedir?
- Sosyal Mühendislik Hedefleri
- Sosyal Mühendislik Saldırıları
- İstatistiksel Veri
- Bilgi Toplama
- Sosyal Mühendisliği Önleme
- Siber Farkındalık: Politikalar ve Prosedürler
- Sosyal Medya
- Modül İncelemesi

11. Yazılım Güvenliği Yazılım Mühendisliği

- Güvenlik Kuralları
- Yazılım Açıkları
- Modül İncelemesi

12. Çevre İzleme

- İzleme
- İzleme ve Kayıt Tutma
- İzleme / Kayıt Tutmanın Faydaları
- Kayıt Tutma
- Metrik
- Modül İncelemesi

13. Fiziksel Güvenlik

- Fiziksel Güvenlik Nedir?
- Derinlemesine Savunma
- Fiziksel Güvenlik Kontrol Çeşitleri
- Cihaz Güvenliği
- İnsan Güvenliği
- Güvenlik Politikaları
- Ekipman İzleme
- Modül İncelemesi

14. Olay Müdahale

- Afet Türleri
- Olay Soruşturmasıyla İlgili İpuçları
- İş Sürekliliği Planlaması
- Felaket Kurtarma Planı
- Adli Olaya Müdahale
- Modül İncelemesi

15. Hukuki Hususlar

- Mevzuata Uygunluk
- Siber Suç
- Modül İncelemesi

16. Siber Güvenlikte Eğilimler

- Siber Güvenlik Tasarım Kısıtlamaları
- Siber İtici Güçler
- Ne Kadar Bağlısın?
- Bağlantıya Ne Kadar Güveniyorsunuz?
- Kimlik Yönetimi
- Siber Güvenlik Standartları
- Siber Güvenlik Eğitimi